REMARKS

Claims 1-35, 69-79 and 88-91 are pending. Claims 36-68 and 80-87 were previously canceled. None of the pending claims have been amended. In light of the following remarks, reconsideration and allowance of the application are respectfully requested.

Interview Summary

Examiner Parthasarathy is thanked for conducting the phone interview on November 12, 2010. The claims were discussed with respect to the pending provisional non-statutory double patenting rejections. It was agreed that a formal response will be submitted to include the arguments presented during the interview.

Provisional Non-Statutory Double Patenting

Claims 1-35, 69-79 and 88-91 stand rejected under the judicially created provisional non-statutory obviousness-type double patenting in view of the copending application no. 11/271,133 ("the '133 application"). The rejections are respectfully traversed.

As an initial matter, MPEP 804 requires that "If a 'provisional' nonstatutory obviousness-type double patenting (ODP) rejection is the only rejection remaining in the earlier filed of the two pending applications, while the later-filed application is rejectable on other grounds, the examiner should withdraw that rejection and permit the earlier-filed application to issue as a patent without a terminal disclaimer." It is noted that the current application was filed on April 8, 2004, which predates the copending '133 application which was filed on November 9, 2005. Moreover, the provisional obviousness-type double patenting rejection is the only rejection remaining in the present application while a final rejection is pending in the later filed '133 application. Thus, under MPEP 804, the provisional obviousness-type double patenting rejection should be withdrawn.

Additionally, the pending provisional obviousness-type double patenting rejection is improper at least because the Office has failed to satisfy the required standard for obviousness-type double patenting rejection, which parallels the guidelines for rejections under 35 U.S.C. § 103(a). (See MPEP § 804.)

A double patenting rejection of the obviousness-type>, if not based on an anticipation rationale,< is "analogous to [a failure to meet] the nonobviousness requirement of 35 U.S.C. 103" except that the patent principally underlying the double patenting rejection is not considered prior art. *In re Braithwaite*, 379 F.2d 594, 154 USPQ 29 (CCPA 1967). Therefore, *>the< analysis employed in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. 103 obviousness determination. *In re Braat*, 937 F.2d 589, 19 USPQ2d 1289 (Fed. Cir. 1991); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985).

Since the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection, the factual inquiries set forth in *Graham v. John Deere Co.,* 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are employed when making an obvious-type double patenting analysis. These factual inquiries are summarized as follows:

(A) Determine the scope and content of a patent claim relative to a claim in the application at issue;

(B) Determine the differences between the scope and content of the patent claim as determined in (A) and the claim in the application at issue;

(C) Determine the level of ordinary skill in the pertinent art; and

(D) Evaluate any objective indicia of nonobviousness.

The conclusion of obviousness-type double patenting is made in light of these factual determinations.

Any obviousness-type double patenting rejection should make clear:

(A) The differences between the inventions defined by the conflicting claims - a claim in the patent compared to a claim in the application; and

(B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue >is anticipated by, or< would have been an obvious variation of >,< the invention defined in a claim in the patent.

(MPEP § 804, II(B)(1)).

Rather than satisfying the four factual inquiries (A)-(D) set forth in *Graham v. John Deere Co.*, the Office merely contends that the claimed limitations in the present application are equivalent to the claims in the copending application. No explanation is given as to why each

claim limitation is obvious in light of the copending application. The following is the entirety of the Office's contention:

1. "obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items are parts of message that were sent over a data network", is analogous to "obtaining routing information from a packet communicated via a network, the routing information including a source address and a destination address", regardless of the wording, further data items are at least "a source and a destination address" (further recited/disclosed in instant dependent claims);
2. "reducing said data item in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item", is analogous to "maintaining a count of packets associated with a device associating with the routing information", regardless of the count of packets still maps to the instant limitation "reduced data item monitoring messages directed to specific computers" as recited and disclosed in instant dependent claims;
3. "analyzing .. . identifying common content indicative of the previously known network attack", is analogous to "identifying the device as a potentially malicious device when the count exceeds a threshold; mapping the source address into a source infected set and mapping the destination address into a destination infected set" and "selectively categorizing the source device associated with the packet as a suspicious device", regardless of the wording, further the claimed instant limitation disclosed explicitly recited in instant dependent claims as "determining a list of first computers that are susceptible to a specified attack";
4. perhaps the only difficult difference that makes use of the alleged invention is "sending the common content to one or more of a signature blocker and a signature manager for use as a new signature in identifying the previously unknown intrusive network attack" vs. "adding the source address to the source infected set and adding the destination address to the destination infected set", the copending claims add the source and destination computers/devices infected set, where as the instant invention further adds the new signature to the list of previously unknown intrusive network attack list.

As seen above, the Office never explains why the mapped limitations are obvious to one of ordinary skill in the art. For example, in (2) above, the claimed limitation requires "reducing said data item in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item." Thus, claim 1 requires reducing said data item in said collection, which is a specific method limitation. Additionally, claim 1 defines the reduced data items in the reduced data collection to

have a smaller size and a constant predetermined relation with data items in the data collection. Thus, a specific relationship between the reduced data collection and the data collection are recited. Moreover, claim 1 requires that at least some of the data items in the data collection that differ are reduced to the same reduced data item. Again, this is a specific act of data reduction. In light of this, it is unreasonable for the Examiner to merely contend that the "reducing..." limitations in claim 1 are analogous to "maintaining a count of packets associated with a device associating with the routing information" in the '133 application. Maintaining a count of packets in the '133 application has nothing to do with the claimed reducing said data items. It is unclear how "maintaining" can be analogous to "reducing said data items."

Moreover, it is unclear what the Examiner intended when contending that "regardless of the count of packets still maps to the instant limitation 'reduced data item monitoring messages directed to specific computers' as recited and disclosed in instant dependent claims." The number of packets is not the issue in claim 1. Claim 1 clearly recites an act of "reducing said data items," rather than a specific number of data items.

Also, the '133 application does not recite any limitation that can reasonably construed as the claimed "wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item." Again, maintaining a count of packets in the '133 patent describes nothing about the size difference between the reduced data items in the reduced data collection and the data items in the data collection. Nor does the maintaining limitation in the '133 patent describe reducing at least some of the data items in the data collection that differ to the same reduced data item.

With respect to (3) above, the claimed limitation at issue recite "analyzing a plurality of said reduced data items to detect common elements in the plurality of said reduced data items, said analyzing identifying common content indicative of the previously unknown network attack." Thus, claim 1 requires analyzing the reduced data items to perform a specific action, namely: "detect comment elements in the plurality of said reduced data items." Additionally, the act of analyzing the reduced data items are further described as "said analyzing identifying common content indicative of the previously unknown network attack." The Office contends that these method limitations are analogous to "identifying the device as a potentially malicious

device when the count exceeds a threshold; mapping the source address into a source infected set and mapping the destination address into a destination infected set" and "selectively categorizing the source device associated with the packet as a suspicious device" in the '133 application. This contention defies logic and common sense for the follow reasons.

First, as described with respect to (2) above, the '133 application does not claim "reducing said data items," which means there are no reduced data items to analyze in the '133 application. Also, the '133 application does not claim "detect[ing] common elements in the plurality of said reduced data items" as required in claim 1 of the present application. Rather, the '133 application recites "identifying the device as a potentially malicious device when the count exceeds a threshold; mapping the source address into a source infected set and mapping the destination address into a destination infected set" and "selectively categorizing the source device associated with the packet as a suspicious device." It is unclear how these limitations of "identifying," "mapping," and "selectively categorizing" could reasonably be construed as detecting common elements. For example, the "identifying" in the '133 application is performed "when the count exceeds a threshold." Clearly, comparing the count to a threshold in the '133 application has nothing to do with detecting common elements. Also, mapping the destination address into destination infected set in the '133 application has nothing to do with detecting common elements. Moreover, selectively categorizing the source device in the '133 application is irrelevant to the claimed detecting comment elements.

With respect to (4) above, the Office concedes that the claimed "sending the common content to one or more of a signature blocker and a signature manager for use as a new signature in identifying the previously unknown intrusive network attack" is different from the claims of the '133 application. Specifically, the Office states that "the copending claims add the source and destination computers/devices infected set, where as the instant invention further adds the new signature to the list of previously unknown intrusive network attack list." In light of this, the Office incorrectly concludes that the claims are analogous because this difference is merely a substitution of what is used to make the detecting/identifying the network attack. This contention is made without any legal or factual support. Moreover, the contention and the underlying reasoning are faulty in their entirety.

As an initial matter, as described with respect to (3) above, the '133 application does not claim detecting common elements. Thus, there are no common elements in the '133 application to send. Also, claim 1 requires a specific act of sending the common elements to one or more of a signature block and a signature manager. This sending is performed to use it as a new signature in identifying the previously unknown intrusive network attack. It is unclear as to how these limitations can reasonably be construed as "adding the source address to the source infected set and adding the destination address to the destination infected set" recited in the '133 application. There are no signature blocks or signature manager recited in the '133 application, and no new signature is used to identify previously unknown intrusive network attack. It is unreasonable to construe the claims of the '133 application as being analogous to the claimed "sending..." when the '133 application fails to recite the claimed signature blocks, signature manager and the new signature.

Moreover, the Office's contention that "it is a merely a substitution of what is used to make the detecting/identifying the network attack" is legally unsupported and defies logic. There are no legal and factual bases to support the Office's contention that such substitution is obvious and not patentably distinct. The Office fails to describe why common sense reasoning would lead one of ordinary skill in the art to make the substitution. Also, if the Office's logic were followed, there would be only one patentable method of detecting network attacks, which is illogical and unsupported by the law.

In addition, the Office is mischaracterizing the claims of the present application and the copending '133 application when contenting that "it is a merely a substitution of what is used to make the detecting/identifying the network attack." Rather, claim 1 of the present application and the claims of the '133 application recite patentably distinct methods of detecting network attacks. For example, claim 1 of the present application expressly recite sending the detected common content to one or more of the signature blocks and a signature manager to use as a new signature in detecting a previously unknown intrusive network attack. Thus, claim 1 analyzes the contents of a message received over the network to obtain reduced data items and analyze the reduced data items to detect common data elements, which can be used as a new signature to indicate previously unknown network attack. In contrast to claim 1 of the present application, the '133 application recites analyzing the address information from the packets received over the

network to identify the source of the network attack. The '133 application does not analyze the contents of the data packets but rather is concerned only with the source of the data packets. Because of at least these differences, the claim mapping presented by the Office is unreasonable and defies common sense reasoning. The table below illustrates the Office's claim mapping.

10/822,226	11/271,133
1. (Currently Amended) A machine-implemented method for automatically identifying new signatures to use in identifying a previously unknown intrusive network attack, comprising:	1. (Currently Amended) A method for detecting malicious attacks, the method comprising:
obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items are parts of messages that were sent over a data network;	obtaining routing information from a packet communicated via a network, the routing information including a source address and a destination address;
reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;	maintaining a cont of packets associated with a device associated with the routing information;
analyzing a plurality of said reduced data items to detect common elements in the plurality of said reduced data items, said analyzing identifying common content indicative of the previously unknown	identifying the device as a potentially malicious device when the count exceeds a threshold; mapping the source address obtained from the packet into a source infected set and mapping the destination address obtained from the

network attack; and	packet into a destination infected set, the mapping comprising: investigating if the source address is in the source infected set; investigating if the source address is also in the destination infected set; investigating if the destination address is in the destination infected set; incrementing an infection count by at least unity when the source address is not in the source infected set and the source address is in the destination infected set; and adding the source address to the source infected set and adding the destination address to the destination infected set; selectively categorizing a source device associated with the packet as a suspicious device.
sending the common content to one or more of a signature blocker and a signature manager for use as a new signature in identifying the previously unknown intrusive network attack.	?

For at least the reasons described above, the provisional obviousness-type double patenting is improper and should be withdrawn.

Rejections under 35 U.S.C. § 112

While the Office Action states that claims are rejected under 35 U.S.C. § 112, it is believe that this was made in error. The Examiner confirmed during the telephonic interview that there are no pending rejections under 35 U.S.C. § 112

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or

other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Pursuant to 37 CFR §1.136, applicant hereby petitions that the period for response to the action dated May 13, 2010, be extended for three months to and including November 15, 2010.

Please apply the required fees in the amount of $555.00, and any charges or credits, to Deposit Account No. 50-5252.

Respectfully submitted,

Date: November 15, 2010

/Hwa C. Lee 59,747/
Hwa C. Lee
Reg. No. 59,747

Perkins Coie LLP
P.O. Box 1247
Seattle, Washington 98111-1247
Telephone: (858) 720-5700
Facsimile: (206) 359-7198